



DEPARTMENT OF THE NAVY
NAVAL INTELLIGENCE COMMAND
2461 EISENHOWER AVENUE
ALEXANDRIA, VA. 22331

CONFIDENTIAL
IN REPLY REFER TO
Ser 44/C133

27 JUL 1977

CONFIDENTIAL

MEMORANDUM FOR THE CHAIRMAN, DIRECTOR OF CENTRAL INTELLIGENCE SECURITY COMMITTEE

Subj: Community-wide adherence to DCID 1/14 (U)

Ref: (a) Director of Central Intelligence Security Committee (C) Memorandum SECOM-D-256 of 12 July 1977

1. (C) Reference (a) advised that the Security Committee has been tasked with reexamining community-wide adherence to DCID 1/14 and requested responses to specific items of inquiry by 30 July 1977.
2. (C) The Navy responses are:

a. Are the investigative standards set forth in DCID 1/14 being met for individuals under consideration for access to SCI? If not, please provide information on which standards are not being met and for what reasons.

Yes, procedurally, the standards are being met. The DCID allows latitude in the provision that "When all other information developed on an individual is favorable, a minor investigative requirement which has not been met should not preclude favorable adjudication." More than ever, minor investigative requirements are not being met because of investigative deficiencies and, sometimes, because of the exigencies of a situation in which the individual must be indoctrinated to perform a function urgently. Advanced technology and a diminishing Navy population combine to intensify the urgency of granting accesses in order to attempt to properly handle, process, utilize and protect increasingly large amounts of intelligence from new, sophisticated, high-volume collection methods.

b. Do you consider the minimum standards high enough to ensure comparability of SCI screening among the Intelligence Community agencies? Should they be revised? Comments and justification for the position you take are requested.

Yes, the standards are high enough. It is questionable whether they are meaningful.



CLASSIFIED BY: DCI SECOP
EXEMPT FROM GDS OF EO 11652
EXEMPTION CATEGORY TWO
DECLASSIFY UPON NOTIFICATION OF ORIGINATOR

CONFIDENTIAL

Navy review completed.

CONFIDENTIAL

CONFIDENTIAL
Ser 44/C133**CONFIDENTIAL**

The standards need to be revised. There is some doubt that the established standards provide a basis by which the security of information now in the custody of personnel can be considered either adequate or cost-effective. Granting access to sensitive compartmented information (SCI) on the basis of present DCID 1/14 investigations often seems to be a waiver of standards.

For example, source restrictions preclude investigative coverage of portions of a person's life. Many local agencies, educational institutions, private organizations and companies withhold information from investigators conducting inquiries for personnel security reasons. Some individual sources have become reluctant to provide information since the Privacy Act was implemented. Economic restraints in the form of resource curtailments imposed on investigative agencies have forced the institution of cost-cutting investigative techniques which result in barely acceptable adherence to the minimum standards. As a result, scope and coverage of investigations are often marginal and logical leads evolving during an investigation are not developed.

A changing political and socio-economic environment, somewhat related to the factors of source restrictions and economic restraints, also contributes to inadequate investigative coverage and challenges the efficacy of the present standards. So-called "transition neighborhoods" allow investigators to rationalize the lack of coverage of areas of residence. An increasingly transient population diminishes the opportunity for investigators to find sources with knowledge of an individual at places of former employment, education or residence. A population more concerned with individual privacy and less concerned with the welfare of neighbors or of the community contributes to less productive investigations. The diminishing population of the Armed Forces requires military personnel to serve more time abroad, on board ships or in other areas of limited accessibility to investigators thus precluding effective investigative coverage of large portions of the backgrounds of some individuals.

In summary, the consequences of source restrictions, economic restraints and a changing environment seem to be a dearth of information. By present standards, access to SCI is granted if the investigation produces no information adversely affecting an individual's loyalty, character and discretion. If an investigation produces little information, a favorable determination still results. With some justification, the present evaluation process has been called "adjudication by exception."

Every adjudication is a risk vs. gain situation in which an attempt is made to predict future human behavior. It follows that an adjudicator must have the greatest amount of valid information about an individual's life and past behavior in order to make the best judgement concerning future reliability. As resources diminish, demand increases and costs rise, it

CONFIDENTIAL

CONFIDENTIAL

Ser 44/C133

CONFIDENTIAL

must be concluded that the ability to economically achieve the necessary information to effectively evaluate personnel in adherence to the investigative standards of DCID 1/14 is diminished to an unacceptable level. It is submitted that security will not be strengthened by perpetuation of antiquated, expensive systems designed to meet yesterday's needs.

In revision, the DCID 1/14 should not require any personnel security criteria unless it has been shown by experience that such are meaningfully productive of information reasonably pertinent to adjudication.

It is suggested that this may be the appropriate time to consider the feasibility of discontinuing the traditional background investigation.

A background investigation would produce more meaningful results by replacement of selected elements with a personal interview conducted by a trained professional; use of a system of applicant testing to assist in predicting future behavior; and, supplemental investigation which would focus on areas of concern developed from the interview, the test results and national and local agency checks as required.

c. Are the reinvestigations of personnel provided access to SCI conducted on a five-year recurrent basis as required by the DCID? If not, what reinvestigation cycle are you currently maintaining? General comments on the programs you have instituted to manage this periodic reinvestigation are also requested.

Yes, Navy reinvestigates every five years. Four and one-half years after completion of a special background investigation, each indoctrinated person is required to resubmit completed statements of personal history on the basis of which reinvestigation is initiated. The SSO at each command or organization monitors the personnel security investigative status of each individual under his accountability. The Navy SSO (Commander, Naval Intelligence Command) supervises the reinvestigation program and takes any necessary action to ensure compliance with the five-year requirement.

d. In addition to security indoctrination, the DCID requires continuing security programs tailored to create mutually supporting procedures under which no issue will escape notice or be left unresolved which brings into question an individual's loyalty and integrity or suggests the possibility of his being subject to undue influence or duress through foreign relationships or exploitable personal conduct. Comments on your security education programs and security supervisory programs are requested. Please include the frequency of these programs, the number of participants in a year, and the estimated cycle for participation in such programs.

Navy SSO personnel, as quotas are available, attend the SSO training program conducted by the Defense Intelligence Agency (DIA). (four (4) SSO staff personnel each calendar year)

CONFIDENTIAL

CONFIDENTIAL**CONFIDENTIAL**

Ser 44/C133

Navy SSO staff personnel attend the SSO training courses sponsored by the Commander, Naval Intelligence Command (COMNAVINTCOM), and conducted by the Fleet Intelligence Training Center, Atlantic, and the Fleet Intelligence Training Center, Pacific. (200 SSO staff personnel each calendar year)

Navy SSO staff personnel are encouraged to visit the Navy SSO at COMNAVINTCOM for orientation, consultation and familiarization with procedures. (25-30 SSO staff personnel each calendar year)

In conjunction with other travel and inspections, the Navy SSO participates in two area SSO conferences each year, one in the Atlantic and one in the Pacific area. (50 SSO staff personnel each calendar year)

A Washington area SSO Conference is scheduled each calendar year and local SSO's are also encouraged to attend annual local area security conferences sponsored by the Security of Military Information Division of the Office of the Chief of Naval Operations. (50 SSO staff personnel each calendar year)

In conjunction with other travel and inspections, the Navy SSO conducts field management visits at SSO facilities as feasible. (50 SSO staff personnel each calendar year)

The training courses, SSO conferences and staff visits all include emphasis on continuing security programs.

The periodically published Navy SSO/SAO Newsletter provides guidance, reminders and admonitions concerning continuing security programs, practices and procedures. (about 700 SSO staff personnel)

The Navy Department Supplement to the DOD Directive S-5200.17 (M-2), Special Security Manual of June 1976, prescribes that security education programs will include the following:

(1) Ensure all personnel assigned to the SSO staff receive the SSO course which is offered by both Fleet Intelligence Training Centers (Atlantic and Pacific).

(2) Individuals who are granted access to sensitive compartmented information must be initially and periodically thereafter indoctrinated as to the unique sensitivity of their position and they must understand the extent of their personal responsibility in safeguarding this material. The recommended reindoctrination interval is two years.

(3) Individuals granted access to SCI should be queried at least annually to ensure that personal history information is kept current. This may be accomplished by a questionnaire or circular distributed to all those having access to SCI.

CONFIDENTIAL

CONFIDENTIAL**CONFIDENTIAL**

Ser 44/C133

The Navy SSO inspects the Commander in Chief, Atlantic Fleet, the Commander in Chief, Pacific Fleet, the Commander in Chief, United States Naval Forces, Europe, the Commander, Naval Security Group Command, the Chief of Naval Material at least every three years. The organizations inspected by the Navy SSO inspect their subordinate SSO's by authority delegated by COMNAVINTCOM. Each inspection includes:

- (1) Examination of the security education and reindoctrination programs in effect,
- (2) examination of the liaison in effect with local authorities and medical personnel,
- (3) a determination of whether periodic reports are received from local authorities in cases of delinquency or misconduct involving Department of Navy military or civilian personnel who are indoctrinated for access to SCI,
- (4) examination of programs which are in effect to indicate excessive indebtedness, repetitive absence, unexplained affluence, excessive use of intoxicants, sexual aberration, criminal or immoral conduct on the part of SCI indoctrinated personnel,
- (5) determination whether the SSO uses all available resources in monitoring activities of SCI indoctrinated personnel to include the use of supervisory security programs.

Inspection of Navy SSO facilities have revealed deficiencies in the pursuit of the continuing security programs which have been recorded and are monitored for compliance. Available resources dictate priorities and operational commitments take precedence over continuing security programs in fleet SSO management.

e. We have been asked to develop an appropriate procedure for the exchange of information to ensure that significant derogatory information used as a basis for denying SCI access by one agency is available to another agency considering granting such access. Your comments on how we might formulate a legal, workable process to effect this exchange is requested.

In the Department of Defense, the results of all investigations conducted by Defense agencies are available through the Defense Central Index of Investigations (DCII). The first step in determining a person's eligibility for access to sensitive compartmented information is inquiry at the DCII to obtain results of any current or former investigation. Any unfavorable information which is part of the person's file will be provided the agency making the request.

CONFIDENTIAL

CONFIDENTIAL**CONFIDENTIAL**

Ser 44/CI33

Obtaining information from non-Defense agencies requires personal liaison efforts by Navy and normally, unfavorable information will not be obtained unless specifically requested or unless another agency coincidentally knows of Navy interest.

There are two possibilities by which such an exchange of information could be established for the Intelligence Community which are offered in the form of recommendations:

(1) It is recommended that a study be made of the feasibility of all NFIB agencies reporting denials of access to the DCII. This would consolidate denial information in an already existing system which now serves all of the Military Departments and the Defense Intelligence Agency.

(2) It is recommended that there be an examination of the feasibility of modification of the proposed Community Computer Compartmentation Control (4C) System to include data indicating unfavorable adjudication of nominees for access to SCI as well as data indicating debrief for cause of formerly indoctrinated personnel. It would seem feasible that the access data program of 4C could be modified to contain such information by addition of a code symbol indicating access denial or termination along with identification of the agency holding the unfavorable information. Such utilization would also serve to increase the cost-effectiveness as well as enhance the security and management applications of the proposed 4C System.



M. C. ANDERSON
Navy Member
Director of Central Intelligence
Security Committee

Copy to:
Navy Member COMIREX
Navy Member SIGINT Committee

CONFIDENTIAL